UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

INTELLECTUAL VENTURES I, LLC, INTELLECTUAL VENTURES II, LLC, Plaintiffs, v. EMC CORP., Defendant.	Civil Action No. 16-10860-PBS LEAD CASE
v. NETAPP, INC., Defendant.	Civil Action No. 16-10868-PBS
v. LENOVO GROUP LTD. and LENOVO (UNITED STATES) INC., Defendants.	Civil Action No. 20-10292-PBS

MEMORANDUM AND ORDER

August 14, 2020

Saris, D.J.

INTRODUCTION

Plaintiffs Intellectual Ventures I, LLC and Intellectual Ventures II, LLC ("IV") have accused three products of infringing U.S. Patent No. 6,968,459 ("the '459 Patent"), the last remaining patent in this protracted litigation. IV accuses

Lenovo's System X servers with self-encrypting drives ("SEDs") of infringing independent claims 15 and 18 and dependent claims 24 and 25 of the '459 Patent, NetApp's storage systems using NetApp Storage Encryption ("NES") of infringing claim 18, and EMC's VNX2 systems with Data at Rest Encryption ("D@RE") Technology of infringing claim 18. Defendants have each brought a separate motion for summary judgment on the basis of non-infringement.

After a consolidated hearing, the Court **ALLOWS** the three motions for summary judgment [Dkt. Nos. 489, 494, 500].

'459 PATENT

The '459 Patent is entitled "Computing environment having secure storage device." As described in the Court's Claim Construction Order, the '459 Patent is a method patent related to data security:

> The '459 patent relates to a method of creating a secure computing environment by "preventing the authorized user from using sensitive data in an unauthorized manner." '459 patent, col. 1, ll. 21-23. With "conventional security measures" prior to the invention claimed in the '459 patent, it was "very difficult to prevent an authorized user from appropriating sensitive data by simply copying the sensitive data to a removable storage device such as a floppy diskette." Id. at col. 1, ll. 23-26. To address this issue, the inventors of the '459 patent developed a computing environment "in which a computer automatically operates in a secure 'full-access' data storage mode when the computer detects the presence of a secure removable storage device." Id. at col. 1, ll. 36-39. Alternatively, "[i]f the computer senses a non-secure removable storage device then the computer automatically operates in a 'restricted-access' mode." Id. at col. 1, ll. 39-42.

Intellectual Ventures I, LLC v. Lenovo Grp. Ltd., No. CV 16-10860-PBS, 2019 WL 4262005, at *1 (D. Mass. Sept. 9, 2019) (hereinafter "Claim Construction Order").

Two independent claims of the '459 Patent are at issue. Those claims read in full:

15. A method for accessing a storage device comprising:

- detecting a storage device within the storage drive;
- sensing whether a storage device has device-specific security information stored thereon;
- providing full-access to the storage device when the storage device has the device-specific security information by:
  - encrypting digital data using the security information during a write access to write the digital data to the storage device; and
  - decrypting digital data using the security information during a read access to read the digital data from the storage device; and
- providing restricted-access to the storage device when the storage device does not store the device-specific security information by preventing the digital data from being written to the storage device during the write access.

18. A method for controlling access to a storage device comprising:

- detecting a storage device within a storage drive;
- sensing whether the storage device has security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user;
- configuring the storage drive to prevent write access to the storage device when the security information is not sensed; and
- configuring the storage drive to permit write access by encrypting digital data using the security information and writing the encrypted digital data

> to the storage device when the security information is sensed.

Dkt. 1-3 at col. 6, ll. 10-27, 36-49.

Figure 1 of the '459 Patent illustrates "a computer that automatically operates in a secure data storage mode when a secure storage device is detected," Id. at col. 2, ll. 6-8:

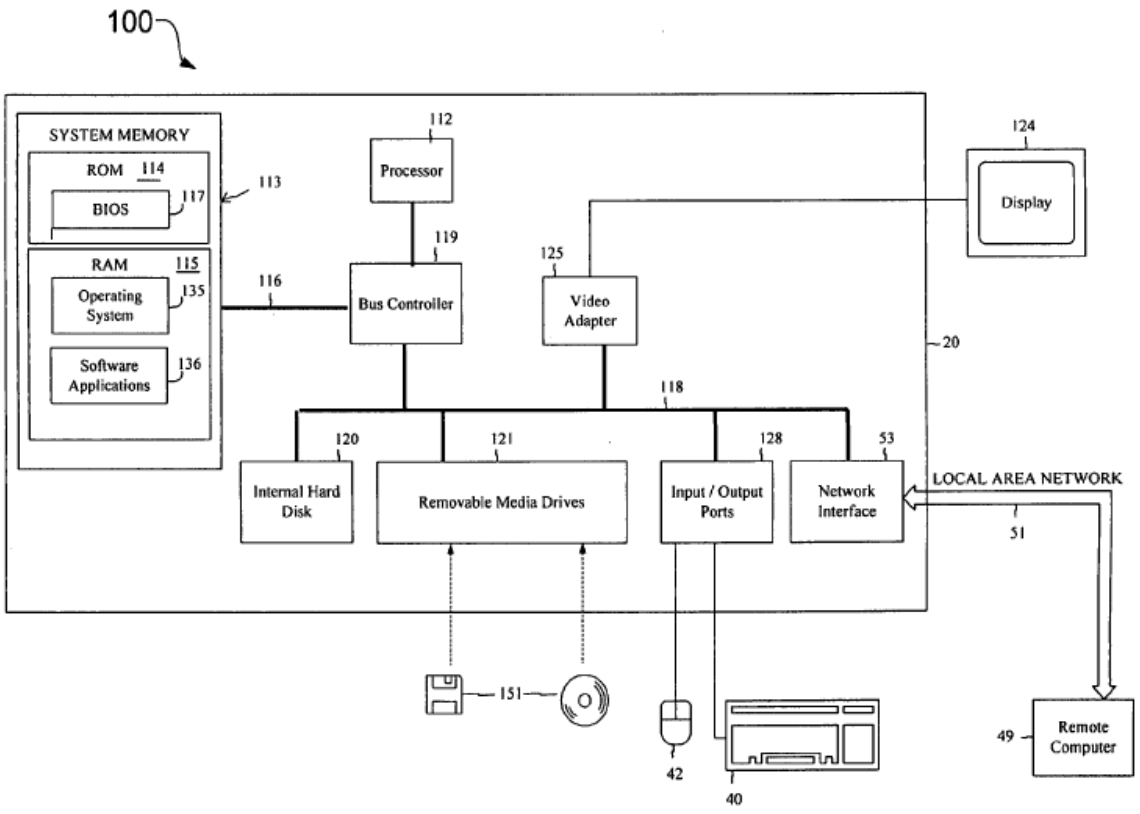


FIG. 1

Id. at 3. The "storage device" in claims 15 and 18 corresponds with figure 151 in this diagram, illustrated by a floppy disk and a CD-ROM, and the "storage drive" with figure 121, labeled "Removable Media Drives."

CLAIM CONSTRUCTION ORDER

This Court held a non-evidentiary Markman hearing and issued its Claim Construction Order on September 9, 2019. At the claim construction stage, the parties disputed the meaning of five terms. The Court gave two terms their plain and ordinary meaning: "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" and "encrypting digital data using the security information." Claim Construction Order, 2019 WL 4262005, at *8.

The Court construed three contested terms: "detecting a storage device within a storage drive," "sensing whether the storage drive has security information," and "device-specific security information." Id. The Court further construed the terms "storage device" and "storage drive" individually. Id.

LEGAL STANDARDS

I. Summary Judgment Standard

Summary judgment is appropriate when there is "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine dispute exists where the evidence "is such that a reasonable jury could resolve the point in the favor of the non-moving party." Rivera-Rivera v. Medina & Medina, Inc., 898 F.3d 77, 87 (1st Cir. 2018) (quoting Cherkaoui v. City of Quincy, 877 F.3d

14, 23-24 (1st Cir. 2017)). "The court must view the facts in the light most favorable to the non-moving party and draw all reasonable inferences in [its] favor." Carlson v. Univ. of New Eng., 899 F.3d 36, 43 (1st Cir. 2018).

II. Infringement Analysis

Analysis of an infringement allegation is a two-step process. First, "the trial court determines the scope and meaning of the asserted claims" in a claim construction order. Searfoss v. Pioneer Consol. Corp., 374 F.3d 1142, 1148 (Fed. Cir. 2004). Second, "the claims as construed by the court are compared limitation by limitation to the features of the allegedly infringing device." Id.

The patent holder bears the burden of proving that the allegedly infringing product satisfies each limitation of the asserted patent claim. Laitram Corp. v. Rexnord, Inc., 939 F.2d 1533, 1535 (Fed. Cir. 1991). Because IV has not alleged infringement under the doctrine of equivalents, it must show literal infringement, meaning "every limitation set forth in a claim must be found in an accused product, exactly." Advanced Steel Recovery, LLC v. X-Body Equip., Inc., 808 F.3d 1313, 1319 (Fed. Cir. 2015) (citation omitted).

Application of a construed claim to the accused product is a "factual determination." Dow Chem. Co. v. United States, 226 F.3d 1334, 1338 (Fed. Cir. 2000). Summary judgment of non-

infringement is nonetheless appropriate where, "on the correct claim construction, no reasonable jury could have found infringement on the undisputed facts or when all reasonable factual inferences are drawn in favor of the patentee." Network, LLC v. Centraal Corp., 242 F.3d 1347, 1353 (Fed. Cir. 2001).

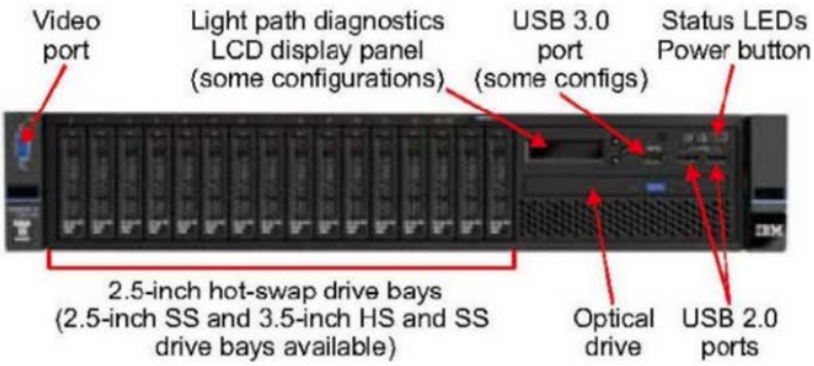
LENOVO'S MOTION FOR SUMMARY JUDGMENT

IV accuses Lenovo's System X servers with self-encrypting drives of infringing independent claims 15 and 18 of the '459 Patent. [1] Lenovo argues that the undisputed evidence demonstrates non-infringement and that, for most of its servers, the claim is barred under the doctrine of patent exhaustion. Because the Court allows summary judgment on the first issue, it does not address the second.

I. Accused Technology

The accused Lenovo System X servers have multiple components including processor(s), storage controller(s), and drive bays. Each drive bay in an accused System X server holds a self-encrypting hard drive ("SED"). This image shows a representative System X server, where the SEDs are held in the drive bay slots across the center left:

[1] IV also accuses the Lenovo products of infringing claims 24 and 25, which are dependent on claim 18. Because the Court concludes Lenovo's products do not infringe claim 18, it need not reach the dependent claims.



LENIV_011335 at 011474

Id. The internal structure of an SED is shown in an image from Lenovo's product documentation:

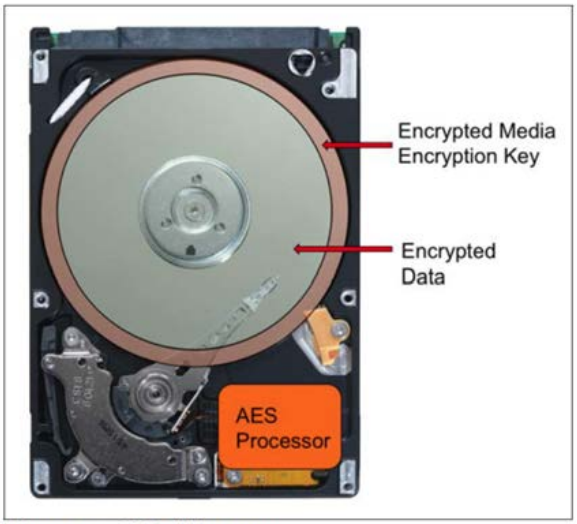


Figure 1-1 SED disk usage

Dkt. 492-3 at 8. Within each SED is a storage medium in the form of a platter, a disk read/write head at the end of an arm that extends over the platter, and components that encrypt and decrypt data. When digital data passes into the SED, it is unencrypted "clear text." Dkt. 492-9 at 35-36. The digital data is then encrypted using a "Media Encryption Key" ("MEK"), which is stored in the copper-toned ring around the platter in the

image above, before it is written to the storage medium in the SED. See Dkt. 492-10 at 17-18; see also Dkt. 492-3 at 52 ("Self-encryption simply means that all of the data written to the storage medium is encrypted by the disk drive before being written and decrypted by the disk drive when it is read.").

II. Parties' Arguments

IV argues that each SED in a Lenovo System X product is a removable storage device and that the storage drive is the "Processor(s), motherboard, Storage controller, Drive bays, and the hardware and software necessary to connect and configure these components." See Dkt. 510-3 at 10. Lenovo disputes that these components are a "storage drive." Dkt. 490 at 14. Lenovo further argues that, even if the components could be considered a "drive," its products do not infringe claim 18 because the components labeled by IV as the "storage drive" are not configured "to permit write access by encrypting digital data." Id. at 16. Rather the SED -- which IV labels as the accused "storage device" -- performs the encryption. Id.

III. Analysis

The relevant limitation in independent claim 18 reads, "configuring the storage drive to permit write access by encrypting digital data using the security information and writing the encrypted digital data to the storage device when

the security information is sensed." Dkt. 1-3 at col. 10, ll. 46-49.

IV argues that this limitation does not require that the storage drive be the component that encrypts digital data or writes the encrypted data. Under IV's reading, the accused drive need only "permit write access" and some other component can perform the necessary encryption. This reading is at odds with the plain text of the limitation, which requires that the storage drive "permit write access by encrypting digital data . . . and writing the encrypted digital data to the storage device." Id. Because it is undisputed that the accused storage device, and not the accused storage drive, "encrypt[s] digital data" and "writ[es] encrypted digital data" within the accused Lenovo products, Lenovo is entitled to summary judgment as to claim 18. See Dkt. 492-3 at 51 (Report by IV's expert Dr. Hugh Smith) ("The MEK is used by the storage device to encrypt all digital data writes." (emphasis added)).

IV argues its expert testimony creates a genuine dispute of material fact on the "encryption" limitation. But IV does not dispute that encryption is performed by components housed within the SED, the accused storage device. Instead, Dr. Smith's opinions regarding infringement rest on the assumption that the storage drive need not be the component that encrypts data. As explained above, that position is contrary to the plain language

of claim 18. "[A] court should discount any expert testimony 'that is clearly at odds with the claim construction mandated by the claims themselves[.]'" Phillips v. AWH Corp., 415 F.3d 1303, 1318 (Fed. Cir. 2005) (en banc) (quoting Key Pharms. v. Hercon Labs. Corp., 161 F.3d 709, 716 (Fed. Cir. 1998)).

IV additionally accuses the Lenovo products of infringing claim 15 of the '459 Patent. The limitation in claim 15 related to encryption reads: "providing full-access to the storage device . . . by . . . encrypting digital data using the security information during a write access to write the digital data to the storage device." Dkt. 1-3 at col. 10, ll. 14-19.

While claim 15 does not require that the storage drive encrypt or write digital data, those functions plainly must be performed by some component other than the storage device. Otherwise, the data would be written by or within the storage device, not "to" it. See id. Lenovo is entitled to summary judgment on claim 15.

NETAPP'S MOTION FOR SUMMARY JUDGMENT

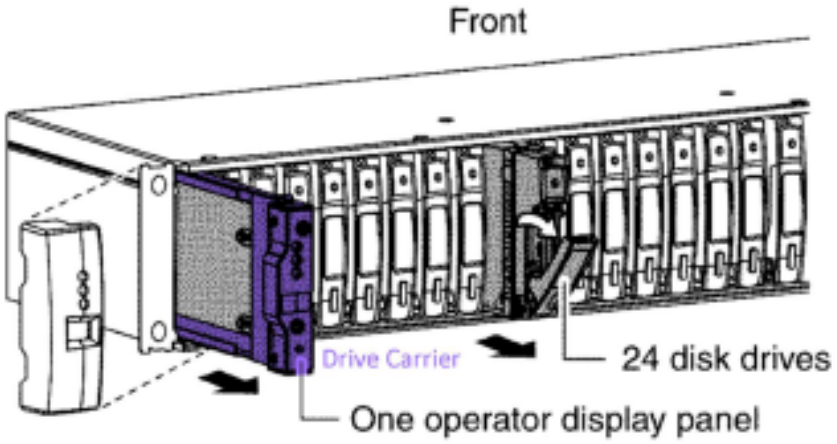
IV accuses certain configurations of NetApp's NSE-enabled servers of infringing independent claim 18 of the '459 Patent.

I. Accused Technology

NetApp's products are accused of infringing the '459 Patent only where the consumer has enabled "NetApp Storage Encryption" ("NSE"), "an optional product feature . . . that offers one

method to prevent unauthorized access to data at rest." Dkt. 495 at 9-10. The accused NetApp products have several components, including a storage controller, which runs a software called "Data ONTAP," and self-encrypting hard disk drives ("SEDs"), which are often held in drive carriers within external disk shelves. The following image depicts a controller with six external disk shelves, which would be connected by cables:

Dkt. 495 at 11; Dkt. 496 ¶ 15. A portion of a single disk shelf is shown below, which depicts a drive carrier being removed on the far left. An SED would be housed within the drive carrier.



Dkt. 497-9 at 23.

The SEDs in the NetApp system contain a storage medium, a drive head that physically reads from and writes to the storage medium, and internal components that encrypt and decrypt data. The encryption/decryption process in the NSE-enabled NetApp products accused of infringement has three steps. In simplified terms, at step one, the controller sends the SED an "authentication key" ("AK"). If the AK from the controller does not match the one stored on the SED, "the SED aborts all access requests." Dkt. 497-9 at 11-12. If the AKs match, the SED decrypts a data encryption key ("DEK") at step two. The unencrypted DEK is then used by the SED to encrypt and decrypt the digital data at step three.

II. Parties' Arguments

IV accuses the NetApp system's controller – including any external disk shelves – as the storage drive in claim 18 and each SED as the storage device.

NetApp first argues the components that IV identifies as the accused "storage drive" in claim 18 are not a "drive." Dkt. 495 at 21. Like Lenovo, NetApp further argues that even assuming those components could constitute a "drive," its products would not infringe claim 18 because they do not meet the limitation for "configuring the storage drive . . . to permit write access . . . by encrypting digital data." Id. at 25. NetApp argues that

the accused storage device -- the SED -- performs the function of encrypting digital data within the NetApp systems, not the accused storage drive.

IV does not respond to this argument in its opposition brief. At hearing, IV reiterated the argument made in regard to Lenovo's motion, which is that claim 18 does not require the storage drive "to be the place where the encryption function is implemented." Dkt. 532 (Transcript) at 93:11. IV agreed at hearing it is undisputed that "the actual encryption algorithm is implemented on the [storage] device" in the accused NetApp systems. Id. at 100:15-101:1.

III. Analysis

Claim 18 includes a limitation for "configuring the storage drive to permit write access by encrypting digital data." Dkt. 1-3 at col. 10, ll. 46-47. The plain text of the limitation requires that the storage drive encrypt digital data as a step of permitting write access. It is undisputed that in the accused NetApp storage systems, the components that perform encryption are housed within the accused storage device -- the SED -- and not the accused storage drive. As such, NetApp is entitled to summary judgment on claim 18.

IV's expert testimony regarding the "encryption" limitation does not create a genuine issue of material fact. Dr. Smith's testimony on the encryption limitation assumes that the storage

drive need not perform the encryption function and so is "'clearly at odds with the claim construction mandated by the claims themselves[.]'" Phillips, 415 F.3d at 1318 (quoting Key Pharms., 161 F.3d at 716).

EMC'S MOTION FOR SUMMARY JUDGMENT

IV accuses EMC's VNX2 systems of infringing claim 18 of the '459 Patent only when used with EMC's add-on Data at Rest Encryption ("D@RE") Technology.

I. Accused Technology

EMC's VNX2 systems have multiple components that form "a refrigerator-sized, array-based storage system," Dkt. 503-1 ¶ 42, represented below in a sample illustration of one possible configuration from EMC's product documentation:

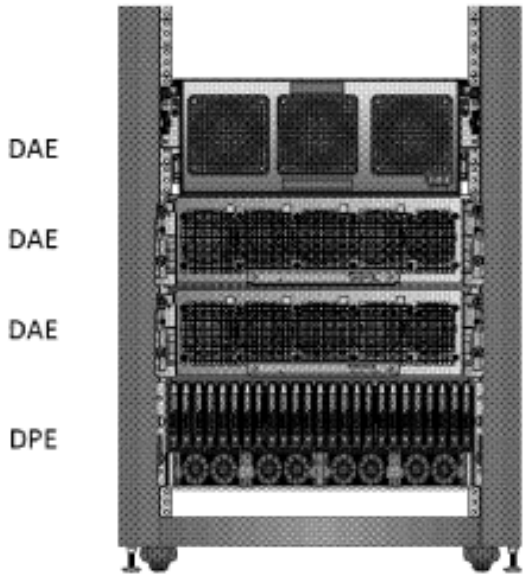


Figure 5. Block dense configuration example

Dkt. 501-7 at 17. This configuration shows a Disk Processor Enclosure ("DPE") and three attached Disk Array Enclosures ("DAE"). Each DAE is akin to a drawer that can be pulled out to access individual disk drives. The VNX2 systems contain up to 1,500 individual disk drives, each of which IV identifies as an accused storage device. The image below shows a "DAE tray extended and open, which reveals the [disk] drives and [cooling] fans." Dkt. 501-7 at 29.

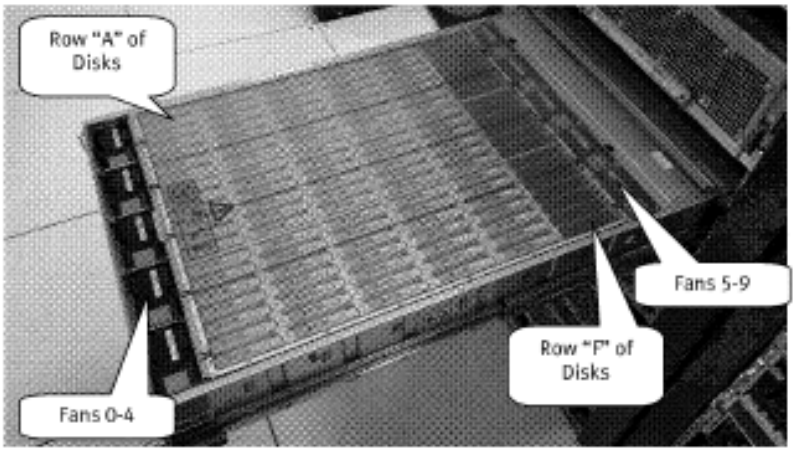


Figure 20. Top of the 120-drive DAE

Each disk drive within a VNX2 system is associated with a particular Globally Unique Identifier ("GUID"). IV accuses the GUID as "the security information" in claim 18, arguing it is "generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user." Dkt. 512-1 at 6. Although the parties dispute how the GUIDs are generated, they agree that a disk drive's GUID is not generated from information related to

individual people who use the VNX2 system, e.g. the individual employees of a company that employs a VNX2 system.

Each VNX2 disk drive includes read/write drive components integrated in a single enclosure along with a storage medium that holds digital data. Unlike the SEDs in the Lenovo and NetApp products, the VNX2's disk drives are not self-encrypting. Instead, when D@RE is activated, data is automatically encrypted or decrypted within the VNX2 controller as it travels between the end-user computers and the disk drives. The data is encrypted using a randomly generated Data Encryption Key ("DEK"), which is unique to each disk drive.

II. Parties' Arguments

EMC argues that its accused products do not infringe claim 18 because they do not "sens[e] security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" and, further, do not "configur[e] the storage drive to permit write access" by "encrypt[ing] digital data using the security information." Dkt. 502-1 at 13, 22-23.

IV accuses the GUID as the infringing "security information." EMC argues that the GUID does not meet this limitation in at least three ways. First, it asserts that the GUID is not generated from "user-specific information associated with a user" because the GUID is unrelated to any individual

user of the VNX2 product, like a particular employee of a company. Second, EMC contends that the GUID cannot be generated from a "combination" of user- and device-specific information, given that no user-specific information is entered. Finally, EMC argues that even if the GUID could be considered "security information," it is not used to encrypt the digital data.

IV responds that the "user" in claim 18 need not be an individual and can instead be "an organization that might 'use' the device through multiple IT professionals charged with its operation." Dkt. 512-1 at 8. Second, it argues that the GUID is generated by RAID software that is associated with an organizational user and therefore meets the combination limitation. Finally, IV contends that claim 18 does not require that the security information serve as the cryptographic key.

III. Analysis

The Court gave the term "security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user" its plain and ordinary meaning. Claim Construction Order, 2019 WL 4262005, at *8.

Citing its expert's testimony, IV asserts that the GUID "is specific to the particular [organizational] user's system" because it is generated "when the user first inserts the storage device into the storage drive and is assigned to a RAID group."

Dkt. 512-1 at 8. RAID ("redundant array of independent disks") software "is designed to perform the RAID function, which is to create an array of independent drives, which allows for redundancy of data in the system." Dkt. 501-27 at 15 (deposition of EMC's technical expert, Thomas Dibb). A system can have one or more RAID "groups." In the VNX2 systems, a system administrator can either manually "select specific drives" to assign to each RAID group or "allow the system to select a set of drives for a RAID group." Id.

IV's expert, Dr. Smith, describes the relationship between the RAID software and the GUID as follows:

> [W]hen a storage device is inserted into the system and assigned to a RAID group, a unique device id (also called a GUID) is generated by the RAID software engine and is written to the storage device. The GUID is used to identify the storage device to the system and is unique to this installation by the user.

Dkt. 513-5 ¶ 19. IV accordingly calls the GUID "installation-specific," which IV equates with "user-specific" because an organizational user determines how to set up its RAID groups. Dkt. 512-1 at 9.

EMC first argues "user-specific information" must be associated with an individual user, not an organization or installation. EMC insists that the specification expressly distinguishes between a "user" of the patented computer system and the "organization" that owns or operates the system. See,

e.g., Dkt. 1-3 at col. 1, ll. 56-58 ("[T]he present invention facilitates the use of a secure storage device as a secure 'access card' by which the user gains access to sensitive data of the organization." (emphases added)); id. at col. 6, ll. 56-60 ("In this manner, an organization can require that all authorized users have a secure storage device 151 in order to access data stored within the organization and to store data on any removable media." (emphases added)). Moreover, the examples given in the '459 Patent of "user-specific information" are all generated from particular individuals. See id. at col. 1, ll. 53-55 (describing how the patented method employs "user-specific information such as a password or biometric information such as input received from a fingerprint scan or retina scan." (emphases added)).

However, a court must not "read limitations from the specification into claims." Thorner v. Sony Computer Entm't Am. LLC, 669 F.3d 1362, 1366 (Fed. Cir. 2012). No party asked the Court to construe the term "user" at the claim construction phase. Its plain and ordinary meaning can encompass both individual and organizational users. Compare user, Random House Webster's College Dictionary, Dkt. 501-19 ("A person or thing that uses something") with user, n.1, Oxford English Dictionary Online, https://www.oed.com/view/Entry/220650 ("A person or organization who makes use of a computer or system"). EMC has

not offered expert testimony that a person of ordinary skill in the art would understand "user-specific" to be limited to exclusively individual users in the context of computers or the '459 Patent specifically.

IV's theory of infringement fails on other grounds, though. To start, IV labels the GUID as "user-specific" by equating "organization-specific" with "installation-specific." While a "user" can be an "organization," there is no evidence that the term extends to a particular "installation."

Moreover, there is no evidence that the GUID is "generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user." Claim Construction Order, 2019 WL 4262005, at *8. The parties seem to agree that at least one input of the GUID is a hard disk drive's serial number, which the Court will assume without deciding qualifies as a form of "device-specific information." EMC contends the serial number is the only input, meaning it is not combined with any user-specific information to generate the GUID.

IV's expert Dr. Smith declared that the GUID meets the "user-specific" limitation because "the GUID is associated with the user (e.g., system owner) at the time of installation and user configuration (i.e., assigning it to a RAID group) because it is created by the RAID software and is specific to the

particular user's system." Dkt. 513-5 ¶ 20. Dr. Smith calls this "consistent with the plain and ordinary meaning of 'user-specific information associated with the user.'" Id. In his report, Dr. Smith similarly says the "RAID software creates a [GUID] . . . using installation specific information (e.g. user-specific information associated with a user)" and calls the GUID "unique to [the] installation." Dkt. 501-24 at 23-24.

Dr. Smith misreads claim 18. The claim requires that the security information be generated from a combination of a device- and user-specific information. Instead, Dr. Smith describes how the GUID is itself associated with a user's installation. Nowhere does Dr. Smith identify the "user-specific information" that is "combined" with the serial number, i.e. device-specific information, to generate the GUID. Indeed, the word "combination" appears only once in Dr. Smith's declaration -- in his recitation of the Court's claim construction. See Dkt. 513-5 ¶ 17.

IV argues the source code discussed by EMC's expert, Dr. Zhao, does not preclude another input beyond the device's serial number. It also argues that since a disk drive's GUID may change if it is installed in a new system, the GUID must be based on some information beyond the serial number. Merely suggesting the GUID might be generated from a user-specific input is not

enough. IV bears the burden of showing the limitation is met. It has failed to do so here.

Finally, EMC argues that, even if the GUID qualifies as "the security information," claim 18 still would not be met because the GUID is not used as an encryption key. It is undisputed that the randomly generated DEK, and not the GUID, is the key that encrypts digital data in the VNX2 systems. Dkt. 513-5 ¶ 32 (Smith Decl.) ("[T]he DEK is doing the actual encrypting of the data that is going to the storage device[.]"). Claim 18 states that the '459 method "configur[es] the storage drive to permit write access by encrypting digital data using the security information." Dkt. 1-3 at col. 10, ll. 46-47. The Court gave the term "encrypting digital data using the security information" its plain and ordinary meaning. Claim Construction Order, 2019 WL 4262005, at *8.

IV argues that the security information does not need to be used as the encryption key but rather can be used at any stage in the encryption process. IV explains that, here, the GUID is "used as part of the encryption process" because the GUID is used to "look[] up" the DEK that is associated with a particular storage device. Dkt. 513-5 ¶ 32.

To support its reading of the limitation, IV points to deposition testimony from EMC's expert Dr. Zhao. Dr. Zhao was asked, "Does Claim 18 require that the security information is

the key?" and he replied, "No; . . . It is sufficient to say that the device itself has what you need in order to retrieve the key in order to decrypt the data that's on the drive." Dkt. 501-29 at 5-6. Later in the deposition, though, he explained he had not heard that the question was specific to claim 18 and clarified that claim 18 "is explicitly saying encrypting digital data using that security information." Id. at 6.

Moreover, "a court should discount any expert testimony that is clearly at odds with the claim construction mandated by the claims themselves." Phillips, 415 F.3d at 1318 (citation omitted). The Court agrees with Dr. Zhao's later explanation of claim 18, which clearly states that the storage drive must "encrypt[] digital data using the security information." Dkt. 1-3 at col. 10, l. 47.

Even if the term "use" were broad enough to encompass IV's proposed meaning, IV has disavowed that broad meaning during the patent's prosecution history. During the IPR proceedings, IV distinguished prior art on the basis that the Petitioner had not shown that "a person of ordinary skill in the art would have used ['security information'] as an encryption key." Dkt. 231-4 at 23; see also Aylus Networks, Inc. v. Apple Inc., 856 F.3d 1353, 1361 (Fed. Cir. 2017) ("[S]tatements made by a patent owner during an IPR proceeding can be considered during claim

construction and relied upon to support a finding of prosecution disclaimer.")

IV also invokes the doctrine of claim differentiation. See Phillips, 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim." (citing Liebel–Flarsheim Co. v. Medrad, Inc., 358 F.3d 898, 910 (Fed. Cir. 2004))). IV points to claims 19 and 24, both dependent on claim 18 but adding the limitations, respectively, "wherein encrypting digital data using the security information comprises generating a cryptographic key as a function of low-level format information for the storage device" and "wherein encrypting digital data using the security information includes generating the cryptographic key as a function of the user-specific information." Dkt. 1-3 at col. 10, ll. 50-53, 64-67. These claims do not preclude a claim construction wherein the security information in claim 18 must be used to encrypt data, but merely provide specific ways to do so. Furthermore, "prosecution history disclaimer can overcome the presumption of claim differentiation." Biogen Idec, Inc. v. GlaxoSmithKline LLC, 713 F.3d 1090, 1097 (Fed. Cir. 2013).

ORDER

The Court **ALLOWS** the motions for summary judgment by the Lenovo Defendants [Dkt. 489], NetApp [Dkt. 494], and EMC [Dkt. 500]. The Court **DENIES AS MOOT** NetApp's motion to strike previously undisclosed infringement theories [Dkt. 458].

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge